September 4, 2014

Weil

Alert
Cyber Security, Cyber Governance, and Cyber Insurance

Cyber Security and Cyber Governance:

Federal Regulation and Oversight – Today and Tomorrow

By Paul A. Ferrillo and David J. Schwartz

In our June 4, 2014 article on cyber security and cyber governance[1] we noted that for many reasons, boards of directors and executives of U.S. companies needed to reexamine how they protect (and respond to the successful hacking of) their most critical intellectual property and customer information. One of the reasons was that all signs out of Washington, D.C. pointed towards increasing federal regulation and oversight of cyber security for public and private companies, and particularly for those in the financial services sector. Further, we foresaw not only heightened scrutiny from regulators, but increasing class action litigation, with plaintiffs accusing boards and management of not taking the appropriate steps to protect company and client data. Our predictions were correct on all fronts.

Just six days after our article, Luis Aguilar, a Commissioner of the United States Securities and Exchange Commission (SEC), stated very clearly in a speech entitled "Cyber Risks in the Boardroom,"[2] that,

> [B]oards must take seriously their responsibility to ensure that management has implemented effective risk management protocols. Boards of directors are already responsible for overseeing the management of all types of risk, including credit risk, liquidity risk, and operational risk **and there can be little doubt that cyber-risk also must be considered as part of board's overall risk oversight**. The recent announcement that a prominent proxy advisory firm [Institutional Shareholders Services (ISS)] is urging the ouster of most of the Target Corporation directors because of the perceived "failure…to ensure appropriate management of [the] risks" as to Target's December 2013 cyber-attack is another driver that should put directors on notice to proactively address the risks associated with cyber-attacks.

Id. (alteration in original) (emphasis added) (footnotes omitted).

Without equivocation, Commissioner Aguilar stated that cyber security was a board responsibility. Likewise, ISS has signaled that directors could or should be held personally accountable for cyber security breaches if they fail to keep their eye on the ball.[3] So too has the plaintiffs' bar recognized that cyber security breaches may become a lucrative addition to their class action litigation practices.[4]

In response to this quickly evolving area of federal regulation and oversight of cyber security, and the ever-increasing scrutiny by multiple constituencies of boards of directors and public companies on cyber security issues, we provide this short, non-exclusive list of how the U.S. government and its agencies are dealing with companies under their specific regulatory authority related to cyber security.[5]

The SEC

Certainly the majority of the federal activity on cyber security issues has come from the SEC. The genesis of its involvement began on or about October 12, 2011, when the SEC issued guidance regarding the disclosure obligations of public companies relating to cyber security risks and cyber incidents. The focus of this guidance was on whether information concerning cyber security and cyber incidents rose to the level of a disclosure obligation either as a risk factor under Regulation S-K Item 503(c) or in the MD&A Section of a Company's mandatory SEC disclosure. One of the critical determining factors for the SEC was whether:

> [T]he costs or other consequences associated with one or more known incidents or the risk of potential incidents represent a **material** event, trend, or uncertainty that is reasonably likely to have a material effect on the registrant's results of operations, liquidity, or financial condition or would cause reported financial information not to be necessarily indicative of future operating results or financial condition.[6]

Id. (emphasis added). If the registrant does determine its cyber security risk or previous cyber incidents rise to the level of a disclosable event, the SEC guidance notes that such disclosure might contain information reflecting:

- Discussion of aspects of the registrant's business or operations that give rise to material cybersecurity risks and the potential costs and consequences;
- To the extent the registrant outsources functions that have material cybersecurity risks, description of those functions and how the registrant addresses those risks;
- Description of cyber incidents experienced by the registrant that are individually, or in the aggregate, material, including a description of the costs and other consequences;
- Risks related to cyber incidents that may remain undetected for an extended period; and
- Description of relevant insurance coverage.

Id.

The SEC's October 2011 cyber guidance was just that – guidance. The question of "materiality" is and was purely left within the discretion of the company. There was no discussion about when the risk of "potential incidents" rose to the level of disclosure. Fueled by continuing major cyber breaches, on March 26, 2014 the SEC organized a "cyber roundtable" among industry groups and public and private sector participants in order to consider, among other things, whether or not additional SEC guidance related to the level of disclosure in a company's public filings was necessary. It will be interesting to see how events develop at the SEC, particularly as cyber breaches continue to increase in number and scope.

SEC Office of Compliance, Inspections and Examinations (OCIE)

On April 15, 2014, the OCIE issued a National Exam Program Risk Alert, entitled "OCIE Cybersecurity Initiative," announcing it would conduct examinations of more than 50 registered broker-dealers and investment advisors "designed to assess cybersecurity preparedness in the securities industry and to obtain information about the industry's recent experiences with certain types of cyber threats."[7] Importantly, this alert came with an extensive list of questions requiring registrants to respond to various areas of their cyber security preparedness. The list requires information such as the registrant's adoption of any "published cybersecurity risk management process standards, such as those issued by the National Institute of Standards and Technology (NIST),"[8] employee training, vendor management, the firm's practices to detect "unauthorized activity on its networks and devices," and specific information, if applicable, concerning any cyber breaches which the registrant experienced since January 1, 2013.

Financial Industry Regulatory Authority (FINRA)

In January 2014, FINRA announced a "sweep" program, similar to OCIE's, whereby firms under FINRA's authority would be receiving targeted examination letters requiring them to respond to questions relating in general to their cyber preparedness.[9] FINRA's targeted examination letters seek very similar information as the OCIE cybersecurity initiative.

Other Federal Regulations Related to Cyber Security

Gramm-Leach Bliley Act (GLBA)

Perhaps most famous for repealing part of the Glass-Steagall Act of 1933, the GLBA, also known as the Financial Services Modernization Act of 1999, has a cyber-data component and applies to "financial institutions," i.e. "any institution engaged in the business of providing financial services to customers who maintain a credit, deposit, trust, or other financial account or relationship with the institution." Under the GLBA, financial institutions are required to "establish appropriate standards" to safeguard a customer's personal financial information, in order: "(1) to insure the security and confidentiality of customer records and information; (2) to protect against any anticipated threats or hazards to the security or integrity of such records; and (3) to protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer."[10] Under the GLBA, financial institutions, in actions brought by the Department of Justice only (there is no private right of action under GLBA), can be fined up to $100,000 for each violation, and directors and officers of financial institutions could be held personally liable for civil penalties of up to $10,000 for each violation.

Payment Card Industry Data Security Standard (PCI DSS)[11]

The PCI DSS is not necessarily a "law" but a list of cyber security standards applied to any U.S. company that processes credit cards, such as a retailer or a financial institution. The list focuses on, among other general requirements, the need to "develop and maintain secure systems and applications," and the need to "track and monitor all access to network resources and cardholder data." These standards provide an "actionable framework for developing a robust payment card data security process – including prevention, detection and appropriate reaction to security incidents."[12] PCI DSS 3.0, adopted in November 2013, enlarges the scope of data security requirements upon retailers and financial institutions.[13] It will be interesting to see whether "3.0," when implemented by retailers, will have any material effect on an industry sector that continues to experience major cyber security breaches along the lines of Target or Neiman Marcus.

Health Insurance Portability and Accountability Act of 1996 (HIPPA)

HIPPA requires, in general, the protection and confidentiality of all electronically protected healthcare information that is created, received, maintained or transmitted. Under HIPPA, a healthcare facility must protect against any reasonably anticipated threat or hazard to the security or integrity of such healthcare information. Under HIPPA, fines can range from $50,000 to $250,000 as well as civil litigation exposure.

Health Information Technology for Economic and Clinical Health Act (the HITECH Act)

The HITECH Act expands the scope of the institutions covered under HIPPA to now include any organization or individual who handles protected healthcare information, which could now include banks, businesses, schools and other organizations.[14]

Today and Tomorrow

Cyber security is the buzzword of the day, year, and maybe the decade. Well-publicized cyber breaches at major U.S. companies are now becoming the norm and have caused not only tremendous anxiety for executives, but reputational damage and material revenue loss for many companies.[15] These breaches have not only caused both consumer and securities class and derivative actions, but have caught the eye

of both federal and state regulators. And Congress will soon get in the game with additional legislation.

In response to this ever changing landscape, directors and officers, and their companies' CISOs and CIOs, must adapt daily, and continue daily discussions about how to improve their company's cyber security procedures and detection/incident response plans of action. Adaptation means real discussion about allocating real physical and financial resources to protect the company's most valuable IP and customer information. Adaptation means that companies and firms need to continue to adopt demonstrable processes and procedures which provide evidence to all constituencies that they are paying attention and responding to the cyber security threat with actionable measures, and not just talking points. Whether that means adopting the NIST cyber security framework or continuing to improve upon their own cyber security procedures in a demonstrable fashion, directors and officers must consider the consequences of failing to act. Even in the face of seemingly unimaginable technological threats (the recent hacking of JPMorgan Chase & Co. by Russian hackers as a possible retaliation for U.S. government sponsored sanctions comes to mind), directors and officers will likely be looked at with ever increasing scrutiny by regulators, customers, and investors.

This article was first published by The D&O Diary *on September 4, 2014.*

1. *See* http://www.dandodiary.com/2014/06/articles/cyber-liability/guest-post-cyber-security-cyber-governance-and-cyber-insurance-what-every-public-company-director-needs-to-know/.
2. *See* http://www.sec.gov/News/Speech/Detail/Speech/1370542057946.
3. *See* Paul Ziobro & Joann S. Lublin, *ISS's View on Target Directors Is a Signal on Cybersecurity*, Wall St. J., May 28, 2014, http://online.wsj.com/articles/iss-calls-for-an-overhaul-of-target-board-after-data-breach-1401285278.
4. *See* Jeffrey Roman, *Supervalu Hit With Lawsuit After Breach*, Bank Info Security (Aug. 20, 2014), http://www.bankinfosecurity.com/supervalu-hit-lawsuit-after-breach-a-7214; *see also* the following recently filed complaints in *Davis v. Steinhafel*, Case Nos. 14-cv-00203-PAM-JJK *et seq*., 2014 WL 3853976 (D. Minn. July 18, 2014) ; *Diana v. Horizon Healthcare Servs., Inc*., Case Nos. 2:13-CV-07418-CCC-MF, 2:14-cv-00584-CCC-MF, 2014 WL 3351730 (D.N.J. June 27, 2014).
5. We leave for another day how various state agencies and authorities (e.g. the New York State Department of Financial Services) are simultaneously dealing with cyber security related issues. *See, e.g*., New York State Department of Financial Services' Report on Cyber Security in the Banking Sector (2014), http://www.dfs.ny.gov/about/press2014/pr140505_cyber_security.pdf.
6. Securities and Exchange Commission, CF Disclosure Guidance: Topic No. 2 (Oct. 13, 2011), http://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm.
7. Office of Compliance Inspections and Examinations, 4 National Exam Program Risk Alert, no. 2, Apr. 15, 2014, http://www.sec.gov/ocie/announcement/Cybersecurity+Risk+Alert++%2526+Appendix+-+4.15.14.pdf.
8. *Id.; see, e.g*., http://www.dandodiary.com/2014/08/articles/uncategorized/guest-post-cybersecurity-and-cyber-governance-understanding-and-implementing-the-nist-cybersecurity-framework/.
9. *See* FINRA, Target Examination Letters re: Cybersecurity (Jan. 2014), http://www.finra.org/industry/regulation/guidance/targetedexaminationletters/p443219.
10. 15 U.S.C. § 6827(4)(a); 15 U.S.C. § 6801(b)(1)-(3).
11. The PCI Security Standards Council is an open global forum for the ongoing development, enhancement, storage, dissemination and implementation of security standards for account data protection. The PCI Security Standards Council's mission is to enhance payment account data security by driving education and awareness of the PCI Security Standards. *See* https://www.pcisecuritystandards.org/.
12. PCI Security Standards Council, Navigating PCI DSS, Understanding the Intent of the Requirements, version 2.0 (Oct. 2010), https://www.pcisecuritystandards.org/documents/navigating_dss_v20.pdf; PCI Security Standards Council, PCI SSC Data Security Standards Overview, https://www.pcisecuritystandards.org/security_standards/ (last visited Aug. 28, 2014).
13. *See* https://www.pcisecuritystandards.org/documents/PCI_DSS_v3.pdf.
14. It should also be noted that federal legislation concerning cyber security has been promulgated to protect government data. The Federal Information Security Management Act was enacted in 2002 namely to "enhance the management and promotion of electronic Government services and processes by establishing a Federal Chief Information Officer within the Office of

Management and Budget, and by establishing a broad framework of measures that require using Internet-based information technology to enhance citizen access to Government information and services." E–Government Act of 2002, Pub. L. No. 107–347, 116 Stat. 2899.

15. For example, Brian Yarbrough, a research analyst with Edward Jones, predicted that after Target's cyber breach, "Probably 5% to 10% of customers will never shop there again." Hadley Malcolm, *Target sees drop in customer visits after breach*, USA Today, Mar. 11, 2014, http://www.usatoday.com/story/money/business/2014/03/11/target-customer-traffic/6262059/.

If you have questions concerning the contents of this issue, please speak to your regular contact at Weil, or to:

Paul A. Ferrillo (NY)	Bio Page	paul.ferrillo@weil.com	+1 212 310 8372
David J. Schwartz (NY)	Bio Page	david.schwartz@weil.com	+1 212 310 8096